Further observations on the distance invariant

Robert S. Coulter

Department of Mathematical Sciences, University of Delaware,
Newark, DE 19716 USA (e-mail: coulter@udel.edu)

Nikolay S. Kaleyski

University of Bergen, 5020 Bergen, Norway (e-mail:
nikolay.kaleyski@uib.no)

Abstract

We adapt an existing lower bound on the Hamming distance between APN functions to the case of planar functions. We compute the exact value of the lower bound for AB and planar functions, and derive an upper bound on the total number of AB and planar functions, respectively, over a given finite field. We use this to conclude that the proportion of AB, resp. planar functions over $\mathbb{F}_{p^n}$ converges to 0 as n approaches infinity.

1 Introduction

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, where p is a prime and n is an arbitrary natural number. An (n,m)**-function** is any function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Any (n,n)-function can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$, where $a_i \in \mathbb{F}_{p^n}$ for $0 \leq i \leq p^n - 1$; this polynomial is called the **univariate representation** of the function, and is uniquely defined. The **algebraic degree** of F is defined as the largest p-weight of any i in $0 \leq i \leq p^n - 1$ with $a_i \neq 0$, where the p-weight $w_p(i)$ of a natural number i is defined to be the sum of the coefficients in the base p expansion of i. Functions of algebraic degree 1, resp. 2 are called **affine**, resp. **quadratic**. An affine function $F(x)$ satisfying $F(0) = 0$ is called **linear**. Linear and affine functions behave in the way that their names would suggest, e.g. $F(x) + F(y) - F(z) = F(x + y - z)$ for any affine (n,n)-function F and any $x, y, z \in \mathbb{F}_{p^n}$.

Set $D_a F(x) = F(x + a) - F(x)$ for any (n,n)-function and any $a \in \mathbb{F}_{p^n}$. For any $a, b \in \mathbb{F}_{p^n}$, let $\delta_F(a,b)$ denote the number of solutions $x \in \mathbb{F}_{p^n}$ to the equation $D_a F(x) = b$. The maximum value of $\delta_F(a,b)$ through all $a \neq 0$ and all b is denoted by δ_F and is called the **differential uniformity** of F. From a cryptographic perspective, δ_F is an important parameter for security considerations as it measures the resistance provided by F against differential cryptanalysis [1]; the lower the differential uniformity, the better. If a function F attains the optimal value $\delta_F = 1$, it is called **perfect nonlinear (PN)** or

planar. Thus an (n,n)-function is PN if and only if $D_aF(x)$ is a permutation for all $a \neq 0$. PN functions can only exist over fields of odd characteristic as, in characteristic 2, $D_aF(x) = D_aF(x+a)$ for all $a \in \mathbb{F}_{p^n}$. The lowest possible value of δ_F for $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is therefore 2, and the functions achieving this optimal value are called **almost perfect nonlinear (APN)**.

Another powerful cryptanalytic attack is linear cryptanalysis [7]; the property measuring the resistance provided by an (n,m)-function against this kind of attack is called nonlinearity. Recall that the **Hamming distance** $d_H(F,G)$ between two (n,m)-functions F and G is $d_H(F,G) = \#\{x \in \mathbb{F}_{p^n} : F(x) \neq G(x)\}$. Fix $p = 2$. The **nonlinearity** of an $(n,1)$-function f is defined as the minimum Hamming distance between f and any affine $(n,1)$-function. The **nonlinearity** $\mathcal{NL}(F)$ of an (n,m)-function F is then the minimum nonlinearity of any component function of F, i.e. any $(n,1)$-function of the form $x \mapsto \mathrm{Tr}(bF(x))$, where $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function. The nonlinearity should be as high as possible, and we know that any (n,m)-function F satisfies $\mathcal{NL}(F) \leq 2^{n-1} - 2^{n/2-1}$ (the so-called *universal bound*). This bound can be achieved with equality only if $m \leq n/2$ [8], and the class of functions attaining it are called **bent**. For (n,n)-functions F, we know $\mathcal{NL}(F) \leq 2^{n-1} - 2^{(n-1)/2}$ (the so-called *SCV bound*) [6, 9]. The class of functions attaining this upper bound are called **almost bent (AB)**. Clearly, AB functions exist only when n is odd. Any AB function is APN, and any quadratic APN function over a field of odd extension degree is AB [5].

The classification of APN and PN functions is considered through equivalence relations that preserve the differential uniformity; typically, these are CCZ-equivalence and EA-equivalence. In the case of quadratic planar functions, we also have isotopic equivalence. We omit the definitions here for the sake of brevity, and refer the reader to [2, 4] for more background on equivalence relations.

A lower bound on the Hamming distance between a given APN function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and any other APN function over $\mathbb{F}_{2^n}$ is given in [3] in terms of the multiset

$$\Pi_F = \{\#\pi_F(b,s) : b, s \in \mathbb{F}_{2^n}\},$$

where $\pi_F(b,s) = \{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n}) F(a+x) + F(x) + F(a+s) = b\}$. It is shown that Π_F is invariant under CCZ-equivalence, and that if we denote by m_F the minimum value occurring in Π_F, then for any APN function G we have $d_H(F,G) \geq \left\lceil \frac{m_F}{3} \right\rceil + 1$. The value is easy to find computationally given a concrete function F, but it appears difficult to determine it theoretically, or to give any meaningful bounds on its value. It is observed that Π_F can take many distinct values across the known APN functions (e.g. 6669 distinct values among the 8180 CCZ-inequivalent APN functions over $\mathbb{F}_{2^8}$ from [10, 11]) which makes it a useful invariant for deciding the CCZ-equivalence of APN functions. In particular, m_F can take many distinct values. A theoretical computation of m_F for $F(x) = x^3$ is given in [3], but even in this simple case the derivation is somewhat technical. Showing that $m_F > 0$ for any APN function F is an open problem, and is directly related to the question of the existence of APN functions over $\mathbb{F}_{2^n}$ of algebraic degree n.

In this paper, we compute the exact value of m_F for all AB and planar functions. We also adapt some of the results of [3], including the lower bound on the Hamming distance, to the case of planar functions. Further, we compute an upper bound on the total number of AB and planar functions over $\mathbb{F}_{p^n}$, and observe that the proportion of such functions goes to 0 as n approaches infinity. Due to space limitations, almost all proofs are omitted.

2 AB functions

We use Theorem 18, p. 276 of [4], and the fact that any AB function is plateaued with single amplitude (Proposition 157, p. 372 of [4]). This is sufficient to compute the exact value of the lower bound for any AB function.

Theorem 1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be plateaued with single amplitude and APN. Then, for any $s \in \mathbb{F}_{2^n}$, we have $\Pi_F = \{(2^{n-1} - 1) \times (2^{2n} - 2^n), 2^n \times 2^n\}$, where $x \times y$ indicates that the value x occurs y times in the multiset.*

In the spirit of the sphere-packing bound, we can now prove the following bound on the number of AB functions.

Corollary 1. *Let n be a natural number. Then there are at most*

$$\frac{(2^n)^{2^n}}{\sum_{i=0}^{d-1} \binom{2^n}{i} (2^n - 1)^i}$$

AB (n, n)-functions, where $d = \frac{2^{n-1}+2}{3}$. In particular, the proportion of (n, n)-AB functions to all (n, n)-functions goes to 0 as n approaches infinity.

3 Planar functions

First, we observe that a fairly straightforward and natural adaptation of the proof of Proposition 2 of [3] leads to a similar result for planar functions.

Proposition 1. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and let $u_1, u_2, \ldots, u_K$ be distinct points from $\mathbb{F}_{p^n}$ for some prime p and some natural numbers n, K. Let $U = \{u_1, u_2, \ldots, u_k\}$ and $a + U = \{a + u : u \in U\}$. Furthermore, if $u_i \in U$ and $a + u_i \in U$, then let $p(i)$ be the index such that $a + u_i = a_{p(i)}$. Finally, let $v_1, v_2, \ldots v_K \in \mathbb{F}_{p^n}$ be arbitrary, and let $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be defined as*

$$G(x) = F(x) + \sum_{i=1}^{K} 1_{u_i}(x) v_i,$$

where $1_{u_i}(x)$ is the indicator function of u_i which evaluates to 0 of $x \neq u_i$ and evaluates to 1 if $x = u_i$. Then G is planar if and only if all of the following conditions are satisfied for any $0 \neq a \in \mathbb{F}_{p^n}$:

(i) $D_a F$ is injective on $\mathbb{F}_{p^n} \setminus (U \cup a + U)$;

(ii) $D_a F(u_i) - D_a F(u_j) \neq v_{p(i)} - v_i - v_{p(j)} - v_j$ for any $u_i \neq u_j$ with $a + u_i \in U$ and $a + u_j \in U$;

(iii) $D_a F(u_i) - D_a F(u_j) \neq v_{p(i)} - v_i - v_j$ for any u_i, u_j such that $u_i + a \in U$ and $u_j + a \notin U$;

(iv) $D_a F(u_i) - D_a F(u_j) \neq -v_i - v_j$ for any $u_i \neq u_j$ such that $u_i + a, u_j + a \notin U$;

(v) $D_aF(u_i) - D_aF(x) \neq v_{p(i)} - v_i$ *for any* u_i, x *such that* $u_i \in U$, $a + u_i \in U$, $x, a + x \notin U$*;*

(vi) $D_aF(u_i) - D_aF(x) \neq -v_i$ *for any* u_i, x *such that* $u_i \in U$, $u_i + a \notin U$, $x, a + x \notin U$*.*

This leads to the following planar function variant of Corollary 1 from [3]. We define $D_a^cF(x) = D_aF(x) - F(a + c)$ for all $a, c \in \mathbb{F}_{p^n}$.

Corollary 2. *Let* F *and* G *be as in the statement of Proposition 1 with* $v_i \neq 0$ *for* $1 \leq i \leq K$*. If* F *and* G *are planar, then for any* i *in* $1 \leq i \leq K$*, no more than* $3K$ *shifted derivatives* $D_a^{u_i}F$ *may map to* $v_i - F(u_i)$*.*

There is also planar function version of Corollary 2 of [3]. For $b, c \in \mathbb{F}_{p^n}$, define $\pi_F(b, c) = \{a \in \mathbb{F}_{p^n} : (\exists x \in \mathbb{F}_{p^n})D_a^cF(x) = b\}$. Set $\Pi_F = \{\#\pi_F(b, c) : b, c \in \mathbb{F}_{p^n}\}$ and $\Pi_F^c = \{\#\pi_F(b) : b \in \mathbb{F}_{p^n}\}$.

Corollary 3. *Let* F *be planar and let* m_F *be the minimum value of an element in* Π_F*. Then*

$$d_H(F, G) \geq \lceil m_F/3 \rceil \tag{1}$$

for any planar function G *over* $\mathbb{F}p^n$*.*

Furthermore, not only can the cardinalities $\#\pi_F(b, c)$ be computed very easily for any planar function, but they can be shown to characterize planar functions.

Proposition 2. *Let* F *be a function over* $\mathbb{F}_{p^n}$*. Then* F *is planar if and only if*

$$\#\pi_F(b, c) = \begin{cases} p^n & b = 0, \\ p^n - 1 & b \neq 0 \end{cases} \tag{2}$$

for any $b, c \in \mathbb{F}_{p^n}$*.*

Proof. By definition, we have $\pi_F(b, c) = \#\{a \in \mathbb{F}_{p^n} : (\exists x \in \mathbb{F}_{p^n})D_aF(x) = F(a + c) + b\}$. Suppose that F is planar. For a fixed a and c, the right-hand side $F(a + c) + b$ is constant; and since D_aF is a permutation for any $a \neq 0$, there exists precisely one $x \in \mathbb{F}_{p^n}$ for which $D_aF(x) = F(a + c) + b$. If $a = 0$, the left-hand side $D_aF(x)$ is equal to 0, and so D_0F maps to $F(c) + b$ if and only if $b = -F(c)$.

Conversely, suppose that (2) holds for F. Let $0 \neq a \in \mathbb{F}_{p^n}$ be some fixed direction; we want to show that D_aF permutes $\mathbb{F}_{p^n}$, which is equivalent to showing that D_aF is surjective. To this end, let $b \in \mathbb{F}_{p^n}$ be arbitrary, and let $b' = b - F(a) = b - F(a + c)$ for $c = 0$. If $b' = -F(0)$, then by (2), there must exist $x \in \mathbb{F}_{p^n}$ for which $D_a^0F(x) = D_aF(x) - F(a) = b' = b - F(a)$, i.e. $D_aF(x) = b$. If $b' \neq -F(0)$, then D_a^0F cannot map to b' for $a = 0$, and by (2) D_a^0F does map to b' for any $a \neq 0$, including the one that we fixed. Once again, we have some $x \in \mathbb{F}_{p^n}$ for which $D_aF(x) = F(a) + b' = b$, and so D_aF is a surjection for any $a \neq 0$. □

Thus, $m_F = p^n - 1$ for any planar F. Consequently, the minimum distance between any two planar functions is at least $d(F, G) \geq \lceil \frac{p^n - 1}{3} \rceil$, which, e.g. for $p = 3$ simplifies to $d(F, G) \geq 3^{n-1}$. This allows us to obtain an upper bound on the number of planar functions over $\mathbb{F}_{p^n}$.

Corollary 4. *Let p, n be natural numbers with p prime. Then the number of planar functions over $\mathbb{F}_{p^n}$ is at most $\frac{(p^n)^{p^n}}{\sum_{k=0}^{d}\binom{p^n}{d}(p^n-1)^d}$, for $d = \lceil \frac{p^n-1}{3} \rceil$. Consequently, the fraction of planar functions over $\mathbb{F}_{p^n}$ to all functions over $\mathbb{F}_{p^n}$ converges to 0 for any prime p as n approaches infinity.*

Using a version of Algorithm 1 from [3], this bound can be shown to be tight computationally for the planar function x^2 over $\mathbb{F}_{3^2}$ and $\mathbb{F}_{3^3}$.

References

[1] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, Jan 1991.

[2] Lilya Budaghyan. *Construction and analysis of cryptographic functions.* Springer, 2015.

[3] Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Nikolay Kaleyski. On the distance between APN functions. *IEEE Transactions on Information Theory*, 66(9):5742–5753, 2020.

[4] Claude Carlet. Boolean functions for cryptography and coding theory. 2021.

[5] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[6] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT 94*, volume 950, pages 356–365, 1994.

[7] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[8] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In *International Workshop on Fast Software Encryption*, pages 111–130, 1994.

[9] V.M. Sidelnikov. On the mutual correlation of sequences. *Soviet Math. Dokl.*, 12:197–201.

[10] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions.

[11] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, codes and cryptography*, 73(2):587–600, 2014.